

**IN THE MATTER OF THE)
SEARCH OF:)
2735 N. FORT AVE.)
SPRINGFIELD, MISSOURI)**

I, Jeffrey Burnett, a Special Deputy with the United States Marshall Service and currently assigned to the Cyber Crimes Task Force (CCTF) with the Federal Bureau of Investigation (FBI), being duly sworn under oath, do hereby depose and state:

2. In the course of my assignment with the FBI, I have participated in the execution of search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of federal laws, including various sections of Title 18, United States Code §§ 2251, 2252 and 2252A involving child exploitation offenses.

Case 6:13-sw-02089-DPR Document 1-1 Filed 12/13/13 Page 1 of 16

experience, my investigation of this matter, and information obtained from other agents and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252(a) and 2252A(a) are located at **2735 N. Fort Ave, Springfield, Missouri** (hereafter referred to as "the Subject Premises").

4. I make this affidavit in support of an application for a search warrant for evidence, fruits, and instrumentalities of the forgoing criminal violations, which relate to the knowing possession, receipt and production of child pornography. The residence to be searched is described in the following paragraphs and in Attachment A. I request authority to search the entire premises, including the residential dwelling, any and all out buildings, vehicles, and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

5. I have probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, 2252 and 2252A, involving the use of a computer in or affecting interstate commerce to receive, possess and produce child pornography, is located in and within the aforementioned residence described below. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits and/or instrumentalities of the aforementioned crimes are located in this residence.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of Title 18, United States Code, §§ 2251, 2252 and 2252A, relating to material involving the sexual exploitation of minors: 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing or coercing a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce, or if

such visual depiction actually was transported in or affecting interstate commerce.

7. 18 U.S.C. § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

The following definitions apply to this Affidavit and its Attachments:

8. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

9. The term "sexually explicit conduct," 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

10. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

11. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or

communications facility directly related to or operating in conjunction with such device.

12. The term “child pornography,” as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where

- a. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
- b. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
- c. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

13. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

14. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

15. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

16. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

17. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

18. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

19. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

20. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

21. The computer's ability to store images in digital form makes the computer itself an ideal

repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

22. The Internet affords individuals several different venues for meeting on another, obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

23. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

24. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.

25. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using

readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

26. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

CELLULAR PHONES AND CHILD PORNOGRAPHY

27. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, cellular phones have likewise revolutionized the manner in which child pornography is produced and distributed.

28. Cellular phones ("cell phones") are exceptionally widespread. The Central Intelligence Agency estimates that in 2009 there were 286 million cell phone subscribers in the United States. Cell phones increasingly offer features such as integrated digital cameras, the ability to store hundreds of digital images and the ability to access and browse the internet.

29. In my training and experience, the ready availability and personal nature of cell phones has led to their frequent use in the commission of child pornography offenses. Individuals with a sexual interest in children will often use their cell phone to browse the internet and to distribute, receive and store child pornography files. Individuals producing child pornography will also

frequently use the integrated digital camera within a cell phone to produce the images, and then store the images both on the phone and on other devices -- such as computers and computer storage media.

30. Cell phones, like other computer systems, will frequently retain data relating to activities, such as Internet browsing history, digital images, and other digital data, that can remain stored for a long period of time.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND CELL PHONES

31. Searches and seizures of evidence from computers and cell phones commonly require agents to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons: Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names.

32. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and are generally difficult to accomplish fully on-site.

33. Searching computer systems and cell phones for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems

and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

34. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

35. Furthermore, because there is probable cause to believe that the computer, its storage devices and cell phones are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

BACKGROUND OF THE INVESTIGATION

36. On 05/13/2013, Homeland Security Investigations Task Force Officer (TFO) Brian Martin was conducting an undercover investigation concerning the distribution of child pornography by suspect(s) using file sharing software, particularly utilizing the ARES network. At approximately 12:45 p.m., a computer using the IP address 50.83.99.107 was observed sharing several images containing suspected child pornography. Utilizing an undercover

computer, TFO Martin was able to make a direct connection with the suspect computer and browse the files available for sharing on the suspect's computer. The computer had at least nine files of interest which appeared to be image and video files, based upon the file name extension.

37. On 05/13/2013, TFO Martin was able to obtain one image file from the suspect computer. The computer was using the ARES software, reporting its version as 2.2.4.3048, and the account was nicknamed "firebird828231@Ares.

38. TFO Martin then reviewed the file received on his undercover computer. The file was named "pthc boys action little boy bedtime jerk off party.jpg", identified by its SHA-1 has value of U3C5L3LUEEZ7K5YZAZICTUKXDPFJN3WC, and is an image file. The picture showed three young males, approximately seven to nine years old. Two males are sitting on what appears to be a bed, touching their penises while a third male stands showing his erect penis to the others.

39. After receiving the file and reports from TFO Martin, I confirmed the image file and its description. The image is consistent with child pornography.

40. On 05/13/2013, TFO Martin requested an Investigative Subpoena from the Barry County, Missouri, Circuit Court requesting the subscriber information for IP address 50.83.99.107 from Mediacom Communications Corporation to determine which subscriber was assigned this IP address on 05/13/2013, between 12:00 p.m. and 1:00 p.m. The response indicated this IP address was assigned to Rachel Neal, 2735 N. Fort Ave, Springfield, Missouri, 65803 during this time period.

41. A public records search for 2735 N. Fort, Springfield, Missouri revealed a Missouri Registered Sex Offender named Alexander Ernest Simmons resides at this address.

42. Using Springfield, MO Police Department resources, I located a police report written on

01/17/2011. Nathan Stowe contacted the police in regards to a past burglary complaint. In the report, Stowe reported he lived with John Barnes, Michele Barnes and Rachel Neal.

43. I was able to identify the following residents:

Alexander Ernest Simmons, white male, date of birth 12/09/1990, social security number 496-04-2143. Missouri Department of Revenue has a listed address of 2735 N. Fort, Springfield, Missouri. Simmons shows a past arrest and conviction for Child Molestation – 2nd Degree.

Nathan Lee Stowe, white male, date of birth 10/27/1988, social security number 493-98-7132. Stowe has a listed address of 120 Fairview Road, Sparta, Missouri with the Department of Revenue. Stowe shows previous arrests for Possession of Controlled Substance and Stealing.

John Carl Barnes, white male, date of birth 08/26/1960, social security number 497-72-0817. Barnes has a listed address of 2735 N. Fort Ave, Springfield, Missouri with the Department of Revenue. Barnes shows past arrests for Passing a Bad Check.

Rachel Jane Neal, white female, date of birth 12/31/1948, social security number 563-64-3440. Neal has a listed address of 2735 N. Fort Ave, Springfield, Missouri with the Department of Revenue. Neal has been arrested in the past for Passing a Bad Check.

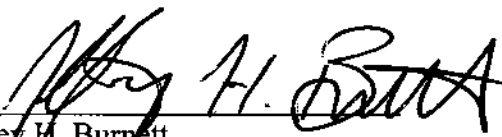
Michele Renee Barnes, white female, date of birth 03/09/1966, social security number 550-08-4402. Barnes shows an address of 2735 N. Fort Ave, Springfield, Missouri with the Department of Revenue. Barnes shows a past arrest for Endangering the Welfare of a Child.

44. A check of the utilities account at the above address shows the account is registered to John Carl Barnes, of birth year 1960; Rachel Jane Neal, date of birth year 1948; and Michele Renee Barnes, birth year 1966. I conducted limited surveillance on **2735 N. Fort Ave, Springfield, Missouri**. I observed a white Jeep Cherokee and a green Dodge pickup. Neither vehicle displayed a license plate. A black Ford Explorer displaying Missouri license plate CL-

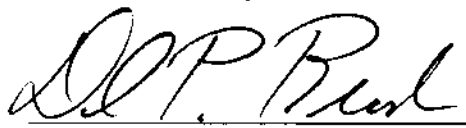
56B checked to a 2010 Toyota and is registered to John Barnes. No unsecured wireless networks were detected in the immediate area and a secured wireless network was available.

PROBABLE CAUSE

45. Based on the above facts, I believe probable cause exists for the issuance of a warrant to search the premises described more fully in Attachment A for (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of a crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means of committing a criminal offense, namely possible violations of Title 18, United States Code, Sections 2251, 2252, and 2252A, including but not limited to the items listed in Attachment B.


Jeffrey H. Burnett
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn before me this th13 day of ~~November~~ December, 2013.


David P. Rush
United States Magistrate Judge
Western District of Missouri

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

The residence to be searched is located at 2735 N. Fort Ave, Springfield, Missouri described as a one, possible two story, single family home. The home is white with white trim and a blue metal roof. The front door is brown and faces east. The numerals "2735" are displayed in black on a white post on the southeast portion of the home.



ATTACHMENT B
Particular Things to be Seized

1. Computers and computer equipment, cellular phones, digital storage devices, tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, flash drives, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, computer software, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners in addition to computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, or other visual depictions of such Graphic Interchange format equipment, and the data stored within these materials, which has been used or may be used for the following:

1) to visually depict minors engaged in sexually explicit conduct, child pornography, and/or child erotica;

2) to advertise, transport, distribute, receive, collect and possess visual depictions of minors engaged in sexually explicit conduct, child pornography, and/or child erotica; and

3) to show or evidence a sexual interest in minors or desire or motive to collect or distribute visual depictions of minors engaged in sexually explicit conduct or child pornography.

2. Records, documents, writings, and correspondence with others pertaining to the possession, receipt, distribution, transportation or advertisement of visual depictions of minors engaged in sexually explicit conduct or child pornography.

3. Any and all photographs, compact disks, DVD's, motion picture films (including but not limited to 8mm film), super 8 video, video cassette tapes, production and reproduction equipment, motion picture cameras, video cameras, video cassette recorders, and other photographic and video recording equipment used to produce or reproduce photographs, motion picture films, or video cassettes, cameras, documents, books, records, ledgers, correspondence, receipts, magazines and other materials reflecting the purchase, sale, trade, transmission, advertising, transport, distribution, receipt and possession of any visual depiction of minors engaged in sexually explicit conduct or to show or evidence a sexual interest in minors or desire or motive to collect, distribute, and receive visual depictions of minors engaged in sexually explicit conduct or child pornography.

4. Any and all magazines, books, photographs, letters, written narratives and computer text files or any other printed or electronic matter to show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect or possess visual depictions of minors engaged in sexually explicit conduct or child pornography.

5. Any and all records showing or bearing indicia of the use, ownership, possession, or control of the residential/business premises described as and items contained therein, including visual depictions of minors engaged in sexually explicit conduct, child pornography, computer equipment, accessories, telephone(s), modem(s), or such records, whether stored on paper, in files, invoices, bills, leases, deeds, permits,

licenses, telephone bills, tax receipts, or other documentation, or on magnetic media such as tape, cassette, disk, diskette or on memory storage devices such as optical disks, or storage media.

6. Envelopes, letters, and other correspondence, including, but not limited to, electronic mail, chat logs, IRC logs, ICQ logs, all usage records for distributed file sharing technologies, and electronic messages, offering to distribute and receive visual depictions of minors engaged in sexually explicit conduct or child pornography, or to show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect and possess visual depictions of minors engaged in sexually explicit conduct or child pornography.

7. Records or other items that evidence ownership or use of computer equipment found in the above residence, including, but not limited to, correspondence, sales receipts, and bills for Internet access, all handwritten notes and handwritten notes in computer manuals.

8. Keys, storage combinations, passwords, and paperwork which indicate any other storage containers or facilities that could contain evidence of collection, advertising, transport, distribution, receipt, or possession of visual depictions of minors engaging in sexually explicit conduct or child pornography.